Multi-dimensional cubic symmetric block cipher algorithm for encrypting big data

Omar A. Dawood1, Othman I. Hammadi2, Khalid Shaker3, Mohammed Khalaf4

1,3Computer Science Department, University of Anbar, Iraq
2College of Education for Humanities Science, University of Anbar, Iraq
4Computer Science Department, Al-Maarif University College, Iraq

ABSTRACT

The advanced technology in the internet and social media, communication companies, health care records and cloud computing applications made the data around us increase dramatically every minute and continuously. These renewals big data involve sensitive information such as password, PIN number, credential numbers, secret identifications and etc. which require maintaining with some high secret procedures. The present paper involves proposing a secret multi-dimensional symmetric cipher with six dimensions as a cubic algorithm. The proposed algorithm works with the substitution permutation network (SPN) structure and supports a high processing data rate in six directions. The introduced algorithm includes six symmetry rounds transformations for encryption the plaintext, where each dimension represents an independent algorithm for big data manipulation. The proposed cipher deals with parallel encryption structures of the 128-bit data block for each dimension in order to handle large volumes of data. The submitted cipher compensates for six algorithms working simultaneously each with 128-bit according to various irreducible polynomials of order eight. The round transformation includes four main encryption stages where each stage with a cubic form of six dimensions.

Keywords:
Big data
Block cipher
Magic cube
Magic square
Symmetric cipher

1. INTRODUCTION

The cryptographic algorithms are a set of rules and mathematical procedures that are used to convert the clear text to an unintelligible text and vice-versa. There are basically two types of the first is cryptographic algorithms of public key cryptography (PKC) or what is called asymmetric cipher where the sender and receiver use two keys one for encryption and the other for the decryption process. The second is secret key cryptography (SKC) also known as symmetric encryption. The symmetric cipher plays an effective role for a trusted block of data where the sender and receiver own the same secret key [1]. The proposed cipher represents a smart step in the designing process of symmetric block cipher construction. The submitted algorithm is dedicated to big data applications and it inherited most of its good characteristics from previously published algorithms [2-4]. Big data refers to the large data sets that increased dramatically and grown continuously from different sources. So the data classified today as the traditional data tomorrow will be big data since the data is evolving without stopping due to the advanced technology of the web applications and the electronic business services [5]. The big data is unlike traditional data because it needs a high potential that outweighs the conventional data from all aspects. So it should take into consideration the designing of a large cipher to meet the growth of data and the cipher should be convenient for the big
volume of data because it became a necessary demand. The big data is not considered new data due to a huge historical data amount created from the earlier time that belongs to deep roots and an extended origin of old data [6]. Big data become a critical issue in recent years as a result of increased the growth of the internet and electronic communications, cloud services and social networks. The amounts of multimedia data generated within social networks are increasing without stopping [7]. Big data has become everywhere and definitely for several application domains. In a big data scenario, the data itself can be mapped to four distinct prototypes: data at rest, data in motion, data in many forms, and data in doubt. Moreover; there exist three forms of data integration in any enterprise: bulk data movement, real-time, and federation [8].

The big data interests with better analysis of the large bulks of data which support more intelligent decision and apply big profitability represented by smart decision, fast decision and impactful decision. Big data has powerful potential for making faster analysis in many scientific disciplines and the success of many enterprises [9]. Since the big data deals with a volume of data is very big and it generates and increases dramatically. Thus it will require a high processing capability compared with the traditional data need. Big data represents an aggregation of data from different kinds that involve current traditional data and an old one, it also includes a mixture of different types of structured and unstructured or multi-structured data that come from various sources [10]. In terms of unstructured data which instantiated from the data set that is not ordered or easily represented by traditional data models. So, social media or what is known as social networks such as Facebook, Tweeter, YouTube and other media from the point of view posts, comments and publications are considered good examples for this type of data. The case of multi-structured data, it indicates diversities of data sorts and formats that can be generated from users and devices, such as current social networks and web services as well as user interactions. The structured data are good examples of big data that may include the combination of text and images in addition to transactional information [11].

There are several distinct block cipher algorithms available that work with different structures and various mathematical descriptions. The present study will focus on the most common symmetric ciphers especially the standard ciphers that involve: IDEA, Triple-DES, AES, Twofish, Serpent, MARS, and RC6. Xuejia Lai and James Massey submitted an International Data Encryption Algorithm (IDEA). It is a new variant of symmetric cipher that was planned to be a replacement for the DES cipher. IDEA cipher encrypts electronic data of 64-bit using a 128-bit ciphering key under the Lai-Massey structure with 8.5 rounds. The IDEA cipher has been analyzed and broken in 2011 via the man in the middle attack and in 2012 full round was cryptanalytic by bicliques attack [12]. IBM Corporation develops Triple DES. It is a revised version for the IBM oldest cipher of data encryption standard (DES) that encrypts the data with a short secret key of 56-bit and Feistel structure. The Triple-DES or 3DES is the three times implementation process for the DES cipher under the length of secret key 168-bit and 48-rounds, although the Triple-DES suffered from the slow implementation it still applying in several civil applications and electronic financial services [13].

National Institute of Standards and Technology (NIST) released the Rijndael cipher as an advance encryption standard (AES) cipher. AES is the name for the block cipher that selected by NIST under the Rijndael name that designed by Vincent Rijmen and Joan Daemen in 1998. The Rijndael block cipher works with SPN structure and encrypts a block of data with a fixed length of 128-bit under three changeable ciphering keys according to the NIST criteria. The AES cipher is inspired by square cipher and is considered the best ciphering model, which is the most widely used algorithm for large scale applications presently [14]. Bruce Schneier et al., designed a Twofish cipher, Twofish is a revision block cipher algorithm for the previous blowfish block cipher. Twofish encrypts a block size of 128 bits and three of different ciphering key reaches 256 bits. It was a finalist candidate to be advanced encryption standard and as an alternated for the 3DES, Twofish algorithm works with 16-rounds of iterated Feistel structure of key-dependent S-Boxes [15]. Ross Anderson et al., designed a Serpent block cipher that is one of the best five finalist symmetric algorithms with SPN structure. Serpent algorithm encrypts the electronic data with a block size of 128-bits and also three different ciphering keys like the AES cipher. The serpent cipher can be implemented in a parallel structure of 32-rounds according to 32-bit of the bit-slices technique [16].

MARS cipher submitted by IBM Corporation, acts a revised cipher for the DES cipher and encrypts the electronic data with block size and key size similar to any AES candidate cipher. MARS encrypts the data via a variable secret key that ranging from 128-bit to 444-bit. MARS characterized by complex structure since it depends on heavy mathematical operations. Thus; it considers the most complicated cipher among the candidates’ algorithms [17]. Rivest et al. [18] designed an RC6 algorithm that considers the simplest and easiest model as the AES candidate algorithm. RC6 cipher represents a revision form of the previous RC5 cipher but with double size. RC6 encrypts the electronic data with block length and a key length of 128-bit and the secret ciphering key can be up to 2040-bit. RC6 designed with Feistel network structure of four words each with 32-bit, which is iterated for 20-rounds completely [18].

In response to the security challenge, the proposed cipher is designed to face real attacks and to solve the traditional security problems in this field. The protection of private and confidential data attracted the researchers’ attention for a long time. So, the basic challenge for the security of big data is data privacy.
The trusted multimedia issues have become critical and necessary in social network and cloud environments because the malicious attacks are becoming more sophisticated and new active malwares have been developed recently [19]. The vulnerability of security systems or fault of security designs can lead to big losses that may exceed even the worst expectations and introduce irreplaceable damage for a company or organization. Since, sensitive data has become accessible from anywhere and the potential of risks for malicious use is made possible. The questions beyond the ethical usage of data and data privacy become momentous. Since big data platforms introduce a broad array of likelihoods to access internal and external data. Unfortunately, most organizations that deal with big data face the same issues of daily threats [20]. Nowadays, most agencies look forward to ensuring that their information are kept securely. So the protect data with all these trends require an appropriate cipher that satisfies the real issues. The developed cipher must defeat the current challenges of end to end encryption, protected user access control, password management and safeguarding internal and external secret information at all levels. Big data terminology needs special cryptographic algorithms with an extended structure of large size or that one with the multi-dimensional cipher of parallel encryption process [21, 22]. The security in such milieu comprises more data stored, which means more security procedures and more modern policies of secrecy that should be taken into consideration to apply the privacy in an effective form. So, “a big question is to what extent the security and privacy technology are adequate for controlled assured sharing for efficient direct access to big data?” [23].

2. RESEARCH METHOD

The proposed cubic cipher works with 16-bytes as a state matrix of 128-bit for each independent face or dimension in the cubic algorithm. Moreover; the cubic algorithm can work with six dimensions together in a parallel form that meaning the data blocks are 6*128-bit. The proposed cipher accepts 128-bits of plaintext from each side in the cube and 128-bits of ciphering secret key as the initial of entry secret key XORed at the first and last rounds according to the whitening concepts. The main operations in the round transformation involve cubic operations with six options according to the cube dimensions. The internal stages for each algorithm aggregated in the round transformation encompass four fundamental stages looped for some rounds. The implementation cubic algorithm as an individual algorithm is subject to the modular arithmetic process. The selected dimension in the cubic algorithm is determined by the least significant byte (LSB) in the ciphering key mod 7 for each round. The result will be less than 7, which represents the dimension number in the cube with range (1-6). Dimension Number (DN)=LSB mod 7. The round transformation of the proposed cipher comprises the following four main stages as stated in Figure 1.

![Figure 1. The cubic algorithm structure](image-url)
2.1. Non-linear black-box stages

This stage is considered the most important part of designing any algorithm which determines the solidity and strength of the algorithm. The proposed black-box consists of six faces or dimensions, whereby each dimension works with the different irreducible polynomial equation as stated in Figures 2-7. The collected dimensions constitute a cube of active black-boxes and each cube face or dimension can be represented as a table lookup of 16*16 values. The intersection of the $i^{th}$ row and $j^{th}$ column in the table for each face gives the desired value. Each Black-box design is constructed similar to the S-Box of AES cipher in terms of taking the multiplicative inverse and applying the affine transform XORed with certain constant vectors of (V1, V2 … V6) as shown in the equations below:

Black-S1[x] = Affine (x^3) + V1  
Black-S2[x] = Affine (x^3) + V2  
Black-S3[x] = Affine (x^3) + V3  
Black-S4[x] = Affine (x^3) + V4  
Black-S5[x] = Affine (x^3) + V5  
Black-S6[x] = Affine (x^3) + V6

Figure 2. Forward black-box1
Figure 3. Forward black-box2
Figure 4. Forward black-box3
Figure 5. Forward black-box4
Figure 6. Forward black-box5
Figure 7. Forward black-box6
2.2. Inverse-non-linear black-box

The inverse Black box stage involves the construction of inverse-cube of six inv-black box lookup tables, where each with 256-bytes and with different irreducible polynomial as stated in Figures 8-13. When the encryption is done by the forward black-box1 the decryption should be by backward inv-black-box1 to ensure the compatibility operations, because the black-box tables are designed with different affine equations, different irreducible polynomials and various constant vectors.

Figure 8. Backward black-box1

Figure 9. Backward black-box2

Figure 10. Backward black-box3

Figure 11. Backward black-box4

Figure 12. Backward black-box5

Figure 13. Backward black-box6

2.3. Internal magic transposition

The Magic transposition acts as the second stage of the round transformation in the proposed algorithm. The main notation beyond the internal magic transposition is to map the values’ positions to other different positions. The magic transposition stage also involves a cube of six dimensions whereby each dimension is arranged according to the doubly even magic square of 4*4 as shown in Figure 14. The magic square of doubly even order is a matrix of (4^m), whereby the order of matrix can be divided by 2 and 4 [24]. The core idea for the design magic cube basically depends on a folded magic square notation that has presented in [25].

Figure 14. Six dimensions of doubly even magic square transposition
2.4. The internal linear matrices stages

The proposed cipher adopts six of new linear MDS codes with their inverses coefficients dedicated for each dimension cube as stated in (7-12). The linear stage is implemented with addition and multiplication operations. The essence mathematical clue is based on Galois field GF ($2^8$) that works separately with each face in the cubic structure. The proposed linear codes can be represented as maximum distance separable (MDS) matrices. The linear MDS matrices code is implemented as a column-by-column multiplication modulo the reducible polynomial of $x^4+1$.

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
04 & 07 & 04 & 06 \\
06 & 04 & 07 & 04 \\
06 & 04 & 06 & 04 \\
07 & 04 & 06 & 04
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
04 & 07 & 04 & 06 \\
07 & 04 & 06 & 04 \\
06 & 04 & 07 & 04 \\
06 & 04 & 07 & 04
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(7)

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
05 & 07 & 05 & 06 \\
06 & 05 & 07 & 05 \\
05 & 06 & 05 & 05 \\
07 & 05 & 06 & 05
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
05 & 07 & 05 & 06 \\
07 & 05 & 06 & 05 \\
06 & 05 & 07 & 05 \\
06 & 05 & 07 & 05
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(8)

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
07 & 05 & 06 & 05 \\
05 & 07 & 05 & 06 \\
06 & 05 & 07 & 05 \\
05 & 06 & 05 & 07
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
07 & 05 & 06 & 05 \\
05 & 07 & 05 & 06 \\
06 & 05 & 07 & 05 \\
05 & 06 & 05 & 07
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(9)

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
04 & 05 & 06 & 06 \\
06 & 04 & 05 & 06 \\
06 & 06 & 04 & 05 \\
05 & 06 & 06 & 04
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
04 & 05 & 06 & 06 \\
06 & 04 & 05 & 06 \\
06 & 06 & 04 & 05 \\
05 & 06 & 06 & 04
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(10)

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
03 & 04 & 01 & 07 \\
07 & 03 & 04 & 01 \\
01 & 07 & 03 & 04 \\
04 & 01 & 07 & 03
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
03 & 04 & 01 & 07 \\
07 & 03 & 04 & 01 \\
01 & 07 & 03 & 04 \\
04 & 01 & 07 & 03
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(11)

$$\begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
03 & 06 & 01 & 05 \\
05 & 03 & 06 & 01 \\
01 & 05 & 03 & 06 \\
06 & 01 & 05 & 03
\end{bmatrix} = \begin{bmatrix}
S_{0,e} \\
S_{1,e} \\
S_{2,e} \\
S_{3,e}
\end{bmatrix} \oplus \begin{bmatrix}
03 & 06 & 01 & 05 \\
05 & 03 & 06 & 01 \\
01 & 05 & 03 & 06 \\
06 & 01 & 05 & 03
\end{bmatrix} = \begin{bmatrix}
S'_{0,e} \\
S'_{1,e} \\
S'_{2,e} \\
S'_{3,e}
\end{bmatrix}$$

(12)

The proposed MDS matrices size is 4*4 like the MDS of AES cipher which is responsible for achieving the confusion and diffusion scheme to the whole structure. The proposed matrices transformations have been chosen from the best solutions we have acquired. The search process for getting the proposed linear equations of order four was computerized automatically. The mathematical software was programmed with Visual Studio C# 2013 under the Windows-10 operating system of 64-bit CPU Intel (R) Core i7 2.65GHz and RAM 8-GB. The inverse MDS matrices linear codes are implemented by using the inverse matrix coefficients in backward operations. All the submitted MDS matrices have been verified as active equations by multiplying the forward matrices by backward matrices. The multiplication result gives the identity matrix for each couple of corresponding matrices. So, the decryption process in each round is implemented by multiplying the Inv-MDS code according to the dimension number with the corresponding encryption MDS code.

2.5. Key addition layer

This is the last stage in the round transformation and the most sensitive stage that determines the strength of the secret ciphering key. The key addition stage involves the key expansion technique for the key generation process that covers all the rounds. The ciphering sub-keys are generated by two complex functions for only one dimension can be shown in Figure 15. Each function consists of three complex operations that increase the complexity of the ciphering key and each one accepts 128-bit of initial entry key. The complex function includes three internal operations of subbyte operation, complement operation and XORed with the constant vector or byte-rotate process. The LSB byte in the ciphering key takes the mod operation for the number seven (mod 7) to determine which face or dimension in the cube through which the encryption process will be implemented in each round.
3. RESULTS AND DISCUSSION

Big data opened the door in front of several sophisticated challenges and numerous information security responsibilities. The proposed cipher can be analyzed from all directions to cover all design details and to figure out the internal operations. The cubic algorithm is designed with a solid round transformation that has six separate paths each of them traverses an independent algorithm. The selection path determines which cube dimension is selected and will be dedicated to encryption. The proposed algorithm adopts a strong secret key that makes the linear and differential attacks very hard. The proposed structure is a composed structure with multi-similar structures that work in parallel simultaneously. Moreover, each algorithm can work as an individual autonomous algorithm. The secret ciphering key is provided with two complex functions that work to prevent the weak/semi-weak sub-keys from appearance through the generation process. The round symmetry for the key scheduling adds an extra layer against the related-key attacks and the square attack. The proposed structure includes six active Black-box tables that apply a high nonlinearity and confusion against the linear and differential attacks. The magic shifting with six dimensions is a new direction for the design secrets with an optimal diffusion to defend the correlation attack. The six different linear MDS codes have been distributed into the proposed cubic dimensions independently. The product cipher with collected stages is affected greatly to the different propagation probabilities of the plaintext and ciphertext for the whole rounds. Furthermore, the product cipher will distribute the number of trails and weights for each bricklayer function iteratively. The differential properties for the algebraic aspects and the multiplicative inverse over Galois Field (GF $2^8$) have been extended for multi-power.

The timing attack becomes impossible for the mathematical internal operations since the algorithm has a balance cubic structure. The balanced structure means that the same implementation time for the encryption and decryption operations in all dimensions. The multiplication process by the MDS code for the linear layer tends to be converged due to equality linear coefficients. The proposed MDS coefficients are almost convergent because they carry the same upper bound of coefficients. Thus, probably there is no leakage information throughout the computation process and consequently, the power analysis attack and timing attacks are very hard. The proposed cipher is focusing on increasing the security layer by preventing the attack from detecting the statistics’ weakness. The ciphering sub-keys are implemented to enhance the security level by encountering all types of cryptanalysis attacks. The proposed cipher adopts an effective strategy for defeating the linear and differential attacks within a multi-dimensional framework. The whole randomness tests released by the National Institute and Standard Technology (NIST) have experimented on the acquired results. The outcome of these tests did not give any fluctuation at randomness boundaries. All of these aspects and tests are taken into account through the designing process. Simple tests for the speed measurement and a number of code lines of the proposed cipher and the original AES is shown in Table 1.

![Figure 15. One dimension key generation algorithm of one-round](image)

<table>
<thead>
<tr>
<th>Algorithm cipher</th>
<th>Block cipher</th>
<th>Key length</th>
<th>No. of rounds</th>
<th>Clock cycle of key scheduling</th>
<th>Clock cycle of encryption process</th>
<th>Code size-assembly language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cubic-dimension1</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12050</td>
<td>13580</td>
<td>10430</td>
</tr>
<tr>
<td>Cubic-dimension2</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12850</td>
<td>13595</td>
<td>10520</td>
</tr>
<tr>
<td>Cubic-dimension3</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12670</td>
<td>13860</td>
<td>10380</td>
</tr>
<tr>
<td>Cubic-dimension4</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12400</td>
<td>14670</td>
<td>10480</td>
</tr>
<tr>
<td>Cubic-dimension5</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12890</td>
<td>14400</td>
<td>10600</td>
</tr>
<tr>
<td>Cubic-dimension6</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>12760</td>
<td>14870</td>
<td>10510</td>
</tr>
<tr>
<td>The standard AES</td>
<td>128-bit</td>
<td>128-bit</td>
<td>10-rounds</td>
<td>11050</td>
<td>12930</td>
<td>9130</td>
</tr>
</tbody>
</table>

**Table 1. Comparison between the proposed model and the original AES**

*Multi-dimensional cubic symmetric block cipher algorithm for encrypting big data (Omar A. Dawood)*
The encryption and decryption implementation time is measured for the proposed cipher according to each dimension independently and compared with the AES standard cipher as shown in Figure 16. The implementation time of the decryption process for the proposed ciphers is varied smoothly from one-dimensional algorithm to another. The time differentiation is occurred due to the coefficients differences in the proposed mathematical equations.

![Implementation Time in Ms](image)

**Figure 16.** Comparison of time implementation encryption/decryption process

4. CONCLUSION

A novel cubic symmetric cipher algorithm has been proposed and developed of round transformation with six dimensions and ten iterated rounds. The proposed cipher has the ability to encrypt the data with multi-dimensional algorithms that compensate for six collected cryptographic algorithms working together. The proposed algorithm includes various mathematical backgrounds of the finite field over GF($2^8$) and magic square mathematical formula. The developed cipher works to encrypt the 128-bit block of data for each dimension independently. Moreover, the main structure can be implemented in parallel from all directions of the cube to increase the speed of the encryption rate in busy servers. The cubic cipher provides a high margin of confidentiality and flexibility in the implementation. The implementation process can be individual or in parallel with a multi-dimensional structure to satisfy the big data needs and the development of technology in different disciplinary fields. The cubic cipher algorithm introduces a modern design structure with accepted results that are almost close to the results of the standard algorithms.

REFERENCES

Multi-dimensional cubic symmetric block cipher algorithm for encrypting big data (Omar A. Dawood)